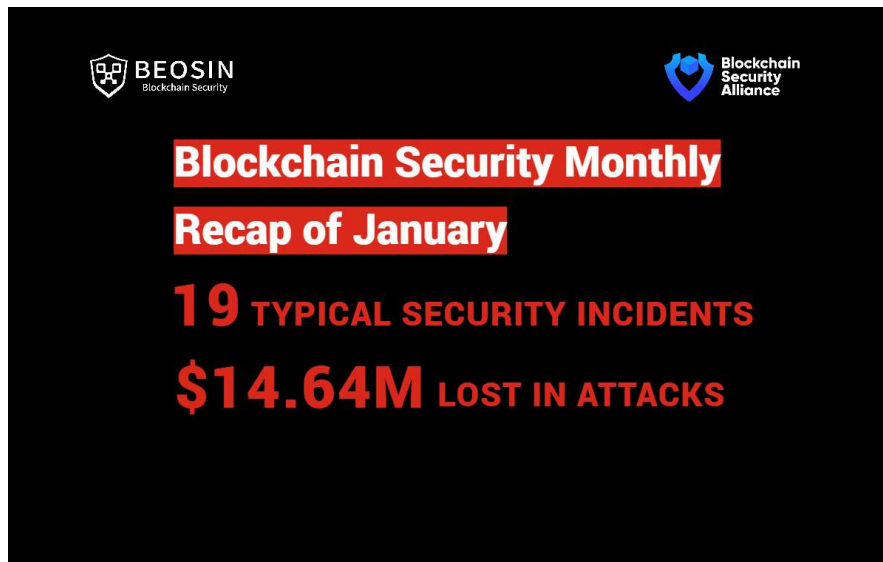February 01, 2023   🔗 Share

Blockchain Security Monthly Recap of January: $14.64M lost in attacks

It's time for our monthly security report! According to Beosin EagleEye security risk monitoring, warning and blocking platform, in January 2023, the number of various security incidents and the amount involved decreased significantly compared with December 2022. In this month, more than 19 typical security incidents occurred and the total loss of various security incidents was about 14.64 million US dollars, which is down about 77% compared with last month and lower than the amount lost in any month in 2022.

The biggest security incident in January was the attack on LendHub, a HECO cross-chain lending platform, which caused a loss of 6 million dolloars because LendHub did not make its old-version contract deprecated. In addition, there were two cases of personal wallet theft and the loss of each case was more than a million dollars. Wallet security still deserves everyone's attention.

DeFi

〖8〗 Typical Security Incidents

№1 On January 10, MetaBankA lost about $13,000 due to a reward miscalculation in its contract.

№2 On January 10, BRA token was attacked due to a logic error in its contract and suffered a loss of $225,000.

№3 On January 12, Roe finance suffered a price manipulation attack, losing about $80,000.

№4 On January 13, LendHub, a HECO cross-chain lending platform, was attacked for not deprecating its old-version contract, with a loss of $6,000,000.
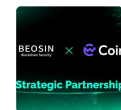

Related Project

**Related Project S
Score**

Learn More

Guess you like

**Web3's Next N
Things to Know**
January 31, 2023

**Beosin and Coir
d Into A Strateg**
February 01, 2023

**A Recap of Beo
NiFT Web3 Sec**
February 02, 2023

**A Great Hit of [
ere will it lead V**
February 03, 2023

**Join the commun
to discuss.**

№7 On January 19, Thoreum Finance was exploited and the amount stolen was about $580,000.

№8 On January 30, Bevo token and StormBringer token were attacked due to the same vulnerability in their contracts with a total loss of $80,000.

NFT

〖2〗 Typical Security Incidents

№1 On January 4, there was a large-scale phishing attack against CryptoPunk, BAYC and other NFTs, which led to the theft of CryptoPunk #4608, CryptoPunk #965, BAYC #1723 and the total loss of these NFTs was worth about $750,000.

№2 On January 28, Azuki, a popular NFT project, confirmed that its Twitter account had been hacked and the confirmed loss was about $780,000.

Wallet Security

〖2〗 Typical Security Incidents

№1 On January 4, a GMX whale wallet was stolen and then the hackers dumped all the GMX token worth of $3,400,000 in the wallet.

№2 On January 26, Kevin Rose, founder of Moonbirds, lost more than $1,000,000 because his personal wallet was hacked.

Rug Pull/Crypto Scam

〖3〗 Typical Security Incidents

№1 On January 11, the contract of ACS token had a backdoor and the contract deployer made a profit of $11,000 after rug pull.

№2 On January 12, CirculateBUSD project had a rug pull through its backdoor and the contract deployer made a profit of about $2,000,000 after rug pull.

№3 On January 20, FFF token was rugged through its backdoor and the contract deployer made a profit of about $1,030,000.

Crypto Crime

〖4〗 Typical Security Incidents

№1 On January 3, Bithumb's former chairman Lee Jung-Hoon has been found not guilty of fraud-related charges by a Seoul Central District Court after a lengthy trial.

№2 On January 6, Aurelien Michel, developer of 'Mutant Ape Planet' NFTs was arrested and charged with fraud for alleged $2.9M rug pull.

№3 On January 14, a coordinated action of Eurojust and Europol has led to the dismantling of a cryptocurrency fraud network operating from Bulgaria, Cyprus and Serbia.

№4 On January 17, The Crown Prosecution Service (CPS) stated that four offenders

In view of the current new situation in the field of blockchain security, Beosin concludes:

Generally, in January 2023, the number of various security incidents and the amount involved decreased significantly compared with December 2022. The total loss of various security incidents was about 14.64 million US dollars, which is lower than the amount lost in any month in 2022.

After the rampant hacking incidents in 2022, the security situation of blockchain in 2023 is relatively stable. Attacks on blockchain projects have been on a downward trend this month while the number of attacks on users' wallets and social media accounts is on the rise. Beosin recommends that users must be aware of phishing, and conduct safe and correct operations on their wallet and social media accounts. The typical rug pulls in this month are rug pulls through backdoor. Thus, users are advised to check projects' audit reports carefully before interacting with them to avoid assets loss.

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, South Korea, Japan and other 10+ countries. With the mission of "Securing Blockchain Ecosystem", Beosin provides "All-in-one" blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 2500 smart contracts including famous Web3 projects PancakeSwap, Uniswap, DAI, OKSwap and all of them are monitored by Beosin EagleEye. The KYT AML are serving 100+ institutions including Binance.

Contact

If you have need any blockchain security services, please contact us:

Website Official Twitter Alert Telegram LinkedIn

Resources

Security Incident

Research Report

Event Update

Partnership Announcement

Resources

Company

About Us

Terms and Conditions

Privacy Policy

Channel Verification

Product&Service

EagleEye

KYT

VaaS

Malicious Websites Identification

Smart Contract Audit

Blockchain Security Audit

Cryptocurrency Tracing

Solution

Compliance

Smart Contract Security

Socials

🐦 Beosin Twitt

🐦 Beosin Alert

✈ Telegram

in Linkedin

Ⓜ Medium

Discord

Stay up-to-date on our latest offerings, tools, and the world of blockchain security.

Contact@beosin.com